

REMARKS

These remarks are responsive to the Office Action, mailed March 15, 2010. Currently claims 1, 3-5, 7-17, and 19-26 are pending with claims 1, 7, and 17 being independent. Claims 2, 6 and 18 have been previously cancelled without prejudice or disclaimer. Claims 1, 5, 7, and 17 have been amended to accommodate Examiner's objections and to expedite prosecution of this application to allowance. No new matter has been added.

Interview

Applicants would like to thank the Examiner for the opportunity to discuss the above application during a telephonic interview held on June 11, 2010 at 1 PM. The following is a summary of the conducted interview.

- (1) no exhibits were discussed or shown at the interview;
- (2) claims 1, 3-17, and 19-26 were discussed;
- (3) U.S. Patent Publication No. 2002/0055972 to Weinman JR (hereinafter, "Weinman"), U.S. Patent No. 5,778,395 to Whiting et al. ("Whiting"), U.S. Patent No. 6,560,615 to Zayas et al. ("Zayas"), U.S. Patent No. 6,847,982 to Parker et al. ("Parker") references were discussed;
- (4) During the interview, Applicants pointed out that the newly cited Weinman reference fails to disclose all elements of the claims, including that based on the criticality of a file, the number of replicas of the file can be increased or decreased in at least one repository. Instead, Weinman simply uses a predefined limit on the number of copies of files to maintain a certain number of such copies across all servers. Weinman also fails to disclose a filter driver that intercepts input or output activity initiated by the client file requests. In contrast, Weinman appears to deal with existing files only and maintaining an appropriate number of copies across its network, rather than intercepting input/output activity initiated by client file requests. Weinman further discloses a corporate policy that simply states that its servers have to be a certain distance away and there should be a minimum number of copies of files distributed in its network. This is different than a protection policy that defines repositories used to protect each share of data. Further, Weinman stores only one copy of file per server, as opposed to storing potentially multiple copies of files in a repository that consists of multiple nodes. Additionally, Weinman fails to have protection policy definitions based on which the filter driver is configured

to capture the snapshot. Weinman does not capture a snapshot, instead, its policy defines a number of copies that should be maintained in the system.

The Examiner and Applicants discussed potential amendments to the currently pending claims in order to expedite prosecution of this application to allowance. During the telephonic interview on June 11, 2010, the Examiner stated that the claims, as currently amended, are allowable over the cited references subject to the Examiner conducting another search.

(5) As stated above, as a result of the interviews, the Examiner and Applicants reached a tentative agreement that claims 1, 3-5, 7-17, and 19-26 are allowable over the currently cited references.

(6) No other matters were discussed during the interview.

35 U.S.C. 103

In the March 15, 2010 Office Action, the Examiner rejected claims 1, 3-5, and 17-25 under 35 U.S.C. 103(a) as being unpatentable in view of various combinations of Weinman, Whiting, and Zayas. Applicants respectfully disagree and traverse these rejections.

Applicants reiterate and incorporate their arguments submitted in their prior Amendments and Responses.

Amended claim 1 recites, *inter alia*, a data protection system, comprising a fileserver configured to contain shares of data and to be in communication with at least one local repository that is in communication with at least one remote repository, wherein two or more repositories are configured to store a replica of a file, wherein each repository includes multiple repository nodes, at least one repository node of each repository is configured to store the replica of the file, wherein a storage location and a number of replicas in each repository is configured to be changed over time by a user. Based on a criticality of the file, the number of stored replicas of the file is increased or decreased in at least one repository. The shares of data are directories or folders of storage capacity created on the fileserver. The fileserver includes a filter driver operative to intercept input or output activity initiated by client file requests, including modification of any existing stored files and/or creation of new files as they occur, and further configured to capture a snapshot of a set of the shares of data at a particular point in time and to maintain a list of modified and/or created files since a last snapshot occurred. The fileserver also

includes a file system in communication with the filter driver and operative to store client files. The fileserver is configured to store a unique protection policy for each share of data on the fileserver. The protection policy defines repositories used to protect each share of data, frequency of data protection, number of replicas of each file that are maintained in each repository, and maintenance of modifications to each share of data. Based on the definitions in the protection policy, the filter driver is configured to capture the snapshot.

As understood by Applicants, Weinman discloses systems and methods for managing data objects in a network such that there may be at least n copies of the data object and each copy of the data object may be separated by at least a distance of d . (Weinman, Abstract). Weinman further discloses a network of servers each storing a copy of an object. (Weinman, para. [0030]). Weinman system knows locations of each of the other copies of the data object and can locate and identify copies that are farther away from a disaster site. (Weinman, para. [0033]). Weinman further defines a corporate policy that presets a minimum number of copies of a data object; alternatively, when an object is created, a user can define a minimum number of copies of the object that must be maintained in the network. (Weinman, para. [0035]). The minimum number of copies can also be correlated with the system's capacity, i.e., a low minimum number can correspond to a system having relatively scarce resources and vice versa. *Id.* Weinman's policy further defines a minimum distance that must separate the copies. (Weinman, para. [0037]). In the event the number of copies of the object falls below a certain number, e.g., deletion of copies, Weinman can appropriately adjust the number of copies. (Weinman, para. [0046]). Weinman system contains information about minimum distance separation, minimum and maximum count requirements, and mappings of copies of an object to locations. (Weinman, para. [0057]).

However, Weinman fails to disclose that based on the criticality of the file, the number of replicas is increased or decreased in at least one repository, as recited in claim 1. Instead, Weinman pre-defines a minimum number of copies that its network of servers must maintain. Weinman does not evaluate whether or not an object is critical and based on that whether or not to increase or decrease the number of its copies. Weinman simply determines whether the number of object copies has fallen below the minimum number because of deletion of copies, server failure, etc., and increases that number appropriately. Criticality of Weinman's objects is irrelevant.

Further, Weinman fails to disclose a filter driver operative to intercept input or output activity initiated by client file requests and configured to capture a snapshot of a set of the shares of data at a particular point in time and to maintain a list of modified and/or created files since a last snapshot occurred, as recited in claim 1. Weinman's system operates with existing objects and pre-defined number of their copies and does not capture a snapshot. Weinman system has knowledge of the number of copies of an object and their locations. This is different than capturing a snapshot.

Weinman's corporate policy is different from the claimed protection policy. The presently claimed protection policy includes information about repositories used to protect each share of data, frequency of data protection, number of replicas of each file that are maintained in each repository, and maintenance of modifications of each share of data, as recited in claim 1. In contrast, Weinman's corporate policy simply defines a minimum number of copies of a particular object to maintain in its network of servers as well as a distance by which such copies must be separated. It does not appear that Weinman's corporate policy defines exactly where to store a copy of an object. This is different from the protection policy of the present invention. Further, according to the presently claimed embodiments, the number and location of replicas in each repository is configured to be changed over time by a user. Weinman does not provide for this in its disclosure.

Weinman fails to capture a snapshot based on the protection policy, contrary to the recitation of claim 1. As stated above, Weinman fails to capture a snapshot, and instead, it simply maintains minimum and maximum numbers of copies of an object and a location of each copy. Weinman's disclosure further does not implement this information to capture a snapshot and as such fails to disclose this element of claim 1.

Further, Weinman's servers store a single copy of an object per server. In contrast, the present invention's repositories include at least one repository node, where each node can store a replica of a file, thus, allowing storage of multiple copies of replicas of files. Hence, if entire Weinman's server system crashes, there will not be a copy left, thereby, making Weinman's system inefficient.

Hence, Weinman fails to disclose, teach or suggest all elements of the claims of the present invention. As such, claim 1 is allowable over Weinman.

Whiting fails to cure the deficiencies of Weinman. As understood by Applicants, Whiting relates to a system for backing up files from disk volumes on multiple nodes of a computer network to a common random-access back storage means. (Whiting, Abstract). Whiting's files are backed up from disk volumes on multiple nodes of a computer network to a single common random-access backup storage means, typically a disk volume. (Whiting, Col. 5, lines 3-6). Thus, Whiting fails to disclose a fileserver configured to contain shares of data and to be in communication with at least one local repository that is in communication with at least one remote repository, wherein two or more repositories are configured to store a replica of a file. There are no multiple repositories that are disclosed in Whiting.

Thus, Whiting performs its backup operations to a single location only and is not equipped to store multiple replicas of a file, which is contrary to the present invention. Whiting teaches away from storing duplicate copies of a file and instead, stores only a single copy of a file. (Whiting, Col. 5, lines 8-11). In fact, Whiting specifically includes a search method that identifies duplicate files and stores only a single copy of the file, thus, it is not capable of storing multiple replicas of the file. Hence, Whiting fails to disclose that two or more repositories are configured to store a replica of a file, wherein each repository includes multiple repository nodes, at least one of which is configured to store the replica of the file, wherein a storage location and a number of replicas in each repository can be configured to change over time, as recited in claim 1. Further, since Whiting backs up its data to the same single location over time, i.e., its \BACKUP\USERS location (Whiting, Col. 7, lines 8-19) and is not capable of storing multiple replicas of files in different locations, it fails to disclose that the number of replicas stored in each repository can be configured to change over time as well, as recited in claim 1.

Applicants respectfully disagree with the Examiner's suggestion that Whiting discloses frequency of data protection as part of a protection policy. Whiting performs backup for all of its files uniformly by "walking" the system. (Whiting, Col. 7, line 59 to Col. 8, line 20). Whiting discovers files that require backup, but does not specify a particular frequency of data protection.

Additionally, Whiting fails to disclose a filter driver operative to intercept input or output activity initiated by client file requests, including modification of any existing stored files and/or creation of new files as they occur, as recited in claim 1. Instead, as stated above, Whiting "walks" the system and looks for changed, new, modified or deleted files, which is a completely

inefficient approach. Whereas, the present invention captures input or output activity as it occurs. Whiting also does not use a protection policy and does not teach capture a snapshot of a set of the shares of data at a particular point in time and to maintain a list of modified and/or created files since a last snapshot occurred, as recited in claim 1.

Like Weinman, Whiting also fails to address criticality characteristic of the files that it backups. Instead, Whiting completely disregards the fact that a file may be critical and number of its replicas may need to be increased so that access to that file can be obtained at any time, especially at the time of system disaster. Instead, it deletes multiple copies of the files regardless of whether or not they are critical. Hence, it fails to disclose, teach or suggest that based on a criticality of the file, the number of stored replicas of the file can be increased or decreased in at least one repository, as recited in claim 1.

Also, similarly to Weinman, Whiting fails to disclose a unique protection policy for each share of data on the fileserver, where the policy defines: repositories used to protect each share of data, frequency of data protection, number of replicas of each file that are maintained in each repository, and, maintenance of modifications to each share of data, as recited in the amended claim 1. Whiting simply deals with storage of data to a single location. Whiting's backup policy is the same for all sets of files, i.e., the policy looks to a set of file to determine which files fall into one of the four categories specified above. This is different than having a protection policy uniquely defined for each share of data on the fileserver, as recited in the amended claim 1. As such, Whiting fails to disclose all elements of the amended claim 1.

Zayas fails to cure the deficiencies of Weinman either alone or in combination with Whiting. As stated in Applicants' prior Amendments and Responses, Zayas appears to relate to backup data and techniques for speeding up backup operations. (Zayas, Col. 1, lines 9-10). When Zayas creates a volume of files, a Modified Files List ("MFL") is established storing a file ID and an epoch timestamp (identifying an important point in time for the volume) is set. (Zayas, Col. 3, lines 38-40). The file ID identifies a file on the volume that has been modified since it was last archived. (Zayas, Col. 5, lines 31-34). Zayas' epoch timestamp identifies the first epoch in which the file identified by file ID was modified since it was last archived. (Zayas, Col. 5, lines 38-40). Zayas further enumerates and orders all identified files in the MFL that were first modified before the selected epoch. (Zayas, Col. 7, lines 16-18).

Zayas fails to disclose that based on a criticality of the file, the number of stored replicas of the file can be increased or decreased in at least one repository, as recited in claim 1. Zayas is simply concerned with creation of its modified file list where files are provided with a file ID and an epoch stamp. As such, it is not concerned with how critical the file can be and whether or not number of replicas for that file need to be increased or decreased.

Zayas also fails to disclose a protection policy that contains definitions recited in claim 1 and that is uniquely defined for each share of data. Zayas is concerned with knowing when a particular file has been modified so that a proper epoch stamp can be applied.

Thus, Weinman, Whiting, Zayas, and/or their various combinations fail to disclose, teach, or suggest all elements of claim 1, and as such, fail to render claim 1 unpatentable, contrary to the Examiner's suggestion. Applicants respectfully request allowance of claim 1.

Claims 3-5 and 17-25 are not rendered obvious by the various combinations of Weinman, Whiting, and/or Zayas for at least the reasons stated above with regard to claim 1. As such, the rejections of claims 3-5 and 17-25 are respectfully traversed. The Examiner is requested to reconsider and withdraw his rejection of claims 3-5 and 17-25.

In the Office Action, the Examiner rejected claims 7-16, 19 and 26 under 35 U.S.C. 103(a) as being unpatentable over various combinations of Weinman, Parker, Zayas, and Whiting. Applicants respectfully disagree and traverse these rejections.

Amended claim 7 recites, *inter alia*, a method for protecting data comprising storing a version of a file within a set of files on a primary disk storage system, capturing a snapshot of the set of files at a particular point in time based on a backup frequency defined in a protection policy, maintaining a list of modified and/or created files since last captured snapshot, examining the protection policy associated with the set of files to determine where and how to protect files associated with the set of files. The protection policy defines repositories used to protect each share of data, frequency of data protection, number of replicas of each file that are maintained in each repository, and maintenance of modifications to each share of data. The method further includes replicating the version of the file to two or more repositories specified by the protection policy, wherein the repositories include at least one of a local repository and a remote repository, wherein a storage location and a number of replicas of the version of the file is configured to be changed over time by a user. Each repository includes multiple repository nodes, at least one

repository node of each repository is configured to store the replica of the file. Based on the criticality of the file, the number of stored replicas of the file is increased or decreased in at least one repository. The protection policy is configured to be uniquely defined for each set of files.

Applicants again reiterate and incorporate their arguments submitted in their previous Amendments and Responses herein by reference in their entirety.

Claim 7 is patentable over Weinman, Zayas, Whiting, and/or their various combinations for at least the reasons stated above with regard to claim 1. Parker fails to cure the deficiencies of Weinman, Zayas, Whiting, and/or their various combinations.

As stated in Applicants previous Amendments and Responses, Applicants understand Parker to disclose an intelligent data inventory and asset management software system. (Parker, Col. 7, lines 18-23). The Parker system includes an Akashic File Clerk that maintains an inventory database, which includes electronic signatures for every file on a work station and all new and changed files. (Parker, Col. 7, line 24-28). Parker allows a client to determine which files are critical and which are not critical, then Parker runs inventories to capture the files that have changed and forwards the changed files to an Akashic Vault for storage and processing. (Parker, Col. 7, lines 28-35). During inventories, Parker identifies files that have 1) changed since the last inventory, 2) been deleted since the last inventory, 3) been added since the last inventory. (Parker, Col. 8, lines 17-26). As such, it appears that Parker, similarly to Whiting, “walks” the system to determine whether there are any files that satisfy any of these three criteria. This is in contrast to the present invention that captures various changes (modification, creation of new files, etc.) as they occur.

Further, Parker’s Akashic Vault is a computer that is attached as a node to the client’s network which stores captured files. (Parker, Col. 7, lines 44-46). After capturing files, Parker’s Vault generates reverse and forward deltas, then deletes the previous version and archives the newest compressed version of the file. (Parker, Col. 9, line 54 to Col. 10, line 4). Parker generates a list of forward delta(s) and copies of the new files and sends them to an offsite Library System. (Parker, Col. 10, lines 5-8). This is different from replicating the version of the file to two or more repositories specified by the protection policy, where the repositories include at least one of a local repository and a remote repository, wherein a storage location and a number of replicas of the version of the file can be configured to change over time, and wherein

each repository includes multiple repository nodes, at least one of which is configured to store the replica of the file, as recited in the amended claim 7.

Parker discloses how files at a client system are check-summed to determine whether their content changes over time and only those files that are new or have changed are sent to the Akashic Vault. (Parker, Col. 7, lines 24-35). In contrast, Parker does not define a unique protection policy for each set of files, where the protection policy defines repositories used to protect each share of data, frequency of data protection, number of replicas of each file that are maintained in each repository, and maintenance of modifications to each share of data, as recited in claim 7.

Additionally, Parker does not provide any disclosure with regard to criticality aspect of files and changing a number of replicas of those files that are considered more or less critical, as recited in claim 7. Instead, Parker is concerned simply with determining whether any kind of changes were made to the files. As such, Parker fails to disclose, teach or suggest all elements of claim 7. Thus, the various combinations of Weinman, Whiting, Parker, and/or Zayas fail to disclose, teach or suggest all elements of claim 7 and Applicants respectfully request allowance of claim 7.

Claims 8-16, 19 and 26 are patentable over various combinations of Weinman, Whiting, Parker, and Zayas for at least the reasons stated above with regard to claim 7. As such, the rejections of claims 8-16, 19 and 26 are respectfully traversed. The Examiner is requested to reconsider and withdraw his rejections of claim 8-16, 19 and 26.

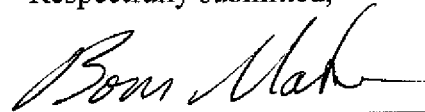
CONCLUSION

No new matter has been added. The claims currently presented are proper and definite. Allowance is accordingly in order and respectfully requested. However, should the Examiner deem that further clarification of the record is in order, we invite a telephone call to the Applicants' undersigned attorney to expedite further processing of the application to allowance.

Applicants believe that no additional fees are due with the filing of this Amendment. However, if any additional fees are required or if any funds are due, the USPTO is authorized to charge or credit Deposit Account Number: **50-0311**, Customer Number: **35437**, Reference Number: **25452-013**.

Date: June 15, 2010

Respectfully submitted,



Boris A. Matvenko, Reg. No. 48,165
Attorney for Applicants
MINTZ LEVIN COHN FERRIS
GLOVSKY & POPEO, P.C.
Chrysler Center
666 Third Avenue, 24th Floor
New York, NY 10017
Tel: (212) 935-3000
Fax: (212) 983-3115